II.   REMARKS

In the Office Action mailed May 09, 2007, the Examiner: (1) rejected claims 1, 11-12, and 17-20 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 6,678,827 to Rothermel et al. (hereinafter "Rothermel"); and (2) rejected claims 2-10 and 13-16 under 35 U.S.C. § 103(a) as being unpatentable over Rothermel in view of U.S. Patent Publication 2002/0087882 by Schneier et al. (hereinafter "Schneier"). Applicants request reconsideration and allowance of the rejected claims in light of the amendments set forth in Section I, *supra*, and the remarks described below.

A.   Explanation of the Claim Amendments

Applicants have amended claims 1, 2, 4, 10-12, 15, and 17-20 to further clarify the claimed invention. The subject matter of the amendments is fully supported by the specification. No new matter has been added.

B.   Response to the 35 U.S.C. § 102(e) Rejections

The Examiner rejected claims 1, 11-12, and 17-20 under 35 U.S.C. § 102(e) as being anticipated by Rothermel. (Office Action, p. 7) Of these claims, claims 1, 11, 17, and 18 are independent. Applicants have amended claims 1, 11, 17 and 18 and submit that the amended claims are allowable over Rothermel for at least the reason that Rothermel does not show or suggest each and every element recited in the claims.

Each of independent claims 1, 11, 17, and 18 includes the concept of a database engine that applies logic reasoning to data from one or more databases to deduce security configuration information for use with configuring security software. This concept is expressed in claim 1 as "the database engine applies logic reasoning to data from a plurality of databases to deduce detailed security rules for network devices based on a general security meta policy for the network," and in claims 11 and 17 as "applying logic reasoning to data from a plurality of databases to deduce one or more security goals for a class of network devices comprising the individual network device, wherein the one or more security goals is based on a general security meta policy for a network comprising the individual network device," and in claim 18 as "using the database engine providing deduction to apply logic reasoning to data from the first and

second databases to deduce one or more security goals for the individual network device, wherein the one or more security goals is based on the general security meta policy."

In contrast to claims 1, 11, 17, and 18, Rothermel describes a Security Policy Manager -- not a database engine -- that combines "the security policy template 300 and the network profile 310 for network 1…to create the security policy 315 for network 1" by replacing "the 'InformationServices' alias in rule 301 with the network addresses listed for the 'InformationServices' alias in definition 311." (Rothermel, col. 10, lines 44-65) Substituting pre-defined values for variables in a template does not show or suggest that "the database engine applies logic reasoning to data from a plurality of databases to deduce detailed security rules for network devices based on a general security meta policy for the network" as recited in claim 1, "applying logic reasoning to data from a plurality of databases to deduce one or more security goals for a class of network devices comprising the individual network device, wherein the one or more security goals is based on a general security meta policy for a network comprising the individual network device" as recited in claims 11 and 17, or "using the database engine providing deduction to apply logic reasoning to data from the first and second databases to deduce one or more security goals for the individual network device, wherein the one or more security goals is based on the general security meta policy" as recited in claim 18. Indeed, Applicants find nothing in Rothermel that discloses a database engine applying logic reasoning to data to deduce configuration information. Accordingly, Applicants submit that claims 1, 11, 17, and 18 are allowable over Rothermel for at least the reason that Rothermel fails to show or suggest each and every element recited in the claims.

Claim 12 depends from claim 11 and claims 19 and 20 depend from claim 18. Accordingly, Applicants further submit that claims 12, 19, and 20 are allowable over Rothermel for at least the reason that they depend from allowable claims.

C.   Response to the 35 U.S.C. § 103(a) Rejections

The Examiner rejected claims 2-10 and 13-16 under 35 U.S.C. § 103(a) as unpatentable over the combination of Rothermel and Schneier. (Office Action, p. 3) Of these claims, claims 4, 10 and 15 are independent. Applicants have amended claims 4, 10, and 15 and submit that the amended claims are allowable over the combination of Rothermel and Schneier for at least the

reason that Rothermel and Schneier do not show or suggest, individually or in combination, each and every element recited in the claims.

Each of independent claims 4, 10, and 15 includes the concept of a database engine that applies logic reasoning to data from one or more databases to deduce security configuration information for use with configuring security software. This concept is expressed in claims 4 and 10 as "database engine applies logic reasoning to data from a plurality of databases to deduce detailed security rules for network devices based on a general security meta policy for the network," and in claim 15 as "applying logic reasoning to data from a plurality of databases to deduce one or more security goals for a class of network devices comprising the individual network device, wherein the one or more security goals is based on a general security meta policy for a network comprising the individual network device."

In contrast to claims 4, 10, and 15, Rothermel describes a Security Policy Manager -- not a database engine -- that combines "the security policy template 300 and the network profile 310 for network 1...to create the security policy 315 for network 1" by replacing "the 'InformationServices' alias in rule 301 with the network addresses listed for the 'InformationServices' alias in definition 311." (Rothermel, col. 10, lines 44-65) Substituting pre-defined values for variables in a template does not show or suggest that a "database engine applies logic reasoning to data from a plurality of databases to deduce detailed security rules for network devices based on a general security meta policy for the network" as in claims 4 and 10, or "applying logic reasoning to data from a plurality of databases to deduce one or more security goals for a class of network devices comprising the individual network device, wherein the one or more security goals is based on a general security meta policy for a network comprising the individual network device." The addition of Schneier fails to overcome the deficiencies of Rothermel because Applicants' can find nothing in Schneier that shows or suggests the claim elements lacking in Rothermel. Accordingly, Applicants submit that claims 4, 10, and 15 are allowable over the combination of Rothermel and Schneier for at least the reason that Rothermel and Schneier do not show or suggest, individually or in combination, each and every element recited in the claims.

Claims 2-3 depend from claim 1, claims 5-9 depend from claim 4, claims 13-14 depend from claim 11, and claim 16 depends from claim 15. Accordingly, Applicants further submit that these claims are allowable for at least the reason that they depend from allowable claims.

III.   Conclusion

Applicants submit that the present application is in condition for allowance, and notice to that effect is hereby requested. Should the Examiner feel that further dialog would advance the subject application to issuance, the Examiner is invited to telephone the undersigned at (312) 913-0001.

Respectfully submitted,

Dated: November 09, 2007   By: /Jeffrey P. Armstrong/
                                                            Jeffrey P. Armstrong
                                                            Reg. No. 54,967